410 Rec'd PCT/PTO 17 SEP 2001

FORM PTO-1390 REV. 2/01T — U S DEPARTMENT OF COMMERCE PATENT AND TRADEMARK OFFICE

TRANSMITTAL LETTER TO THE UNITED STATES DESIGNATED/ELECTED OFFICE (DO/EO/US) CONCERNING A FILING UNDER 35 U.S.C. 371

ATTORNEY'S DOCKET NUMBER
07904.0052
Customer No.: 22,852

U.S. APPLICATION NO.
(If known, see 37CFR1.5)
09/936615

INTERNATIONAL APPLICATION NO.	INTERNATIONAL FILING DATE	PRIORITY DATE CLAIMED
PCT/EP00/02414	March 17, 2000	March 18, 1999

TITLE OF INVENTION: **METHOD OF SECURING DATA IN A PORTABLE MASS MEMORY AGAINST UNAUTHORIZED DUPLICATION**

APPLICANT(S) FOR DO/EO/US
Wolfgang NEIFER

Applicant herewith submits to the United States Designated/Elected Office (DO/EO/US) the following items and other information:

1. ☒ This is a **FIRST** submission of items concerning a filing under 35 U.S.C 371.
2. ☐ This is a **SECOND** or **SUBSEQUENT** submission of items concerning a filing under 35 U.S.C. 371.
3. ☐ This is an express request to begin national examination procedures (35 U.S C. 371(f)). The submission must include items (5), (6), (9) and (21) indicated below.
4. ☒ The US has been elected by the expiration of 19 months from the priority date (Article 31).
5. ☒ A copy of the International Application as filed (35 U.S.C. 371 (c)(2)).
   a. ☐ is attached hereto (required only if not communicated by the International Bureau.
   b. ☒ has been communicated by the International Bureau.
   c. ☐ is not required, as the application was filed with the United States Receiving Office (RO/US).
6. ☒ An English language translation of the International Application as filed (35 U.S.C. 371 (c)(2)).
   a. ☒ is attached hereto.
   b. ☐ has been previously submitted under 35 U.S.C. 154 (d)(4).
7. ☒ Amendments to the claims of the International Application under PCT Article 19 (35 U.S.C. 371 (c)(3)).
   a. ☐ are attached hereto (required only if not communicated by the International Bureau).
   b. ☐ have been communicated by the International Bureau.
   c. ☐ have not been made; however, the time limit for making such amendments has NOT expired.
   d. ☒ have not been made and will not be made.
8. ☐ An English language translation of the amendments to the claims under PCT Article 19 (35 U.S.C. 371 (c)(3)).
9. ☒ An oath or declaration of the inventor(s) (35 U.S.C. 371 (c)(4)).
10. ☒ An English language translation of the annexes of the International Preliminary Examination Report under PCT Article 36 (35 U.S.C. 371 (c)(5)).

Items 11 to 20 below concern document(s) or information included:

11. ☐ Information Disclosure Statement under 37 CFR 1.97 and 1.98
12. ☒ An assignment document for recording. A separate cover sheet in compliance with 37 CFR 3.28 and 3.31 is included.
13. ☐ A FIRST preliminary amendment.
14. ☐ A SECOND or SUBSEQUENT preliminary amendment.
15. ☐ A Substitute specification.
16. ☐ A change of power of attorney and/or address letter.
17. ☐ A computer-readable form of the sequence listing in accordance with PCT Rule 13ter.2 and 35 U.S.C. 1.821-1.825.
18. ☐ A second copy of the published international application under 35 U.S.C. 154 (d)(4).
19. ☐ A second copy of the English language translation of the international application 35 U.S.C. 154 (d)(4).
20. ☒ Other items or information:
   a. ☒ Copy of cover page of International Publication No. WO 00/55707.
   b. ☐ Copy of Notification of Missing Requirements.
   c. ☐

09936615 091701

U.S. APPLICATION NO. (If known, see 37CFR 1.5) 09/936615	INTERNATIONAL APPLICATION NO. PCT/EP00/02414	ATTORNEY'S DOCKET NUMBER: 07904.0052

21. ☒ The following fees are submitted:

CALCULATIONS PTO USE ONLY

BASIC NATIONAL FEE (37 CFR 1.492 (a) (1) - (5)):

Neither international preliminary examination fee (37 CFR 1.482) nor international search fee (37 CFR 1.445(a)(2)) paid to USPTO and International Search Report not prepared by the EPO or JPO **$1000.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search Report prepared by the EPO or JPO **$860.00**

International preliminary examination fee (37 CFR 1.482) not paid to USPTO but International Search fee (37 CFR 1.445(a)(2)) paid to USPTO **$710.00**

International preliminary examination fee (37 CFR 1.482) paid to USPTO but all claims did not satisfy provisions of PCT Article 33(1)-(4) **$690.00**

International preliminary examination fee (37 CFR 1.482) paid to USPTOand all claims satisfied provisions of PCT Article 33 (1)-(4) **$100.00**

				ENTER APPROPRIATE BASIC FEE AMOUNT =	$860.00	
Surcharge of $130.00 for furnishing the oath or declaration later than ☐ 20 ☐ 30 months from the earliest claimed priority date (37 CFR 1.492 (e)).					$	
CLAIMS	NUMBER FILED		NUMBER EXTRA	RATE		
Total Claims	22	- 20 =	2	x $18.00	$36.00	
Independent Claims	1	-3 =		x $80.00	$	
MULTIPLE DEPENDENT CLAIM(S) (if applicable)				+$270.00	$270.00	
				TOTAL OF THE ABOVE CALCULATIONS =	$1166.00	
☐ Applicant claims small entity status. See 37 CFR 1.27. The fees indicated above are reduced by ½.					$	
				SUBTOTAL =	$1166.00	
Processing fee of **$130.00** for furnishing the English translation later than ☐ 20 ☐ 30 months from the earliest priority date (37 CFR 1.492(f)).					$	
				TOTAL NATIONAL FEE =	$1166.00	
Fee for recording the enclosed assignment (37 CFR 1.21 (h)). The assignment must be accompanied by an appropriate cover sheet (37 CFR 3.28, 3.31). **$40.00** per property. +					$40.00	
				TOTAL FEES ENCLOSED =	$1206.00	
					Amount to be refunded:	$
					charged:	$

a. ☐ A check in the amount of $ 1206.00 to cover the above fees is enclosed.

b. ☐ Please charge my Deposit Account No. _____ in the amount of $ _____ to cover the above fees. A duplicate copy of this sheet is enclosed.

c. ☒ The Commissioner is hereby authorized to charge any additional fees which may be required, or credit any overpayment to Deposit Account No. 06-0916. A duplicate copy of this sheet is enclosed.

d. ☐ Fees are to be charged to a credit card. **WARNING:** Information on this form may become public. **Credit card information should not be included on this form.** Provide credit card information and authorization on PTO-2038.

NOTE: Where an appropriate time limit under 37 CFR 1.494 or 1.495 has not been met, a petition to revive (37 CFR 1.137 (a) or (b)) must be filed and granted to restore the application to pending status.

SEND ALL CORRESPONDENCE TO:

Finnegan, Henderson, Farabow, Garrett & Dunner, L.L.P.
1300 I Street, N.W.
Washington, D.C. 20005-3315
EFC/FPD/sci
DATED: September 17, 2001

SIGNATURE

Ernest F. Chapman/25,961

NAME/REGISTRATION NO.

JC16 Rec'd PCT/PTO SEP 17 2001

4/prts

A Method of Securing Data in a Portable Mass Storage against Unauthorized Copying

The invention relates to a method of securing data in a portable mass storage against unauthorized copying and a replay system for performing the method.

Multimedia contents and software are quite predominantly disseminated commercially on data carriers which can be written to only once and constitute the trade product together with the contents stored thereon. A separate commercial dissemination of the contents independent of such data carriers would in principle be possible, for instance by remote access to networks including a payment function, but fails because of a lack of protection against unauthorized copying.

The invention provides a method of securing data in a portable mass storage against unauthorized copying, which can be performed with little expenditure and using available technology. In accordance with the method of the invention the data is first stored in the mass storage in a scrambled form. In a replay system for the data at least one SAM module (Safe Access Module) is used which has stored thereon a personal identity code of an authorized user. The descrambling keys required for descrambling the data are stored on the SAM module of the authorized user. Assigned to the data is an authorization code which is stored on the SAM module. Then an authorization code encoded by means of the personal identity code is formed on the SAM module. This encoded authorization code is stored on the mass storage with the scrambled data. Prior to a replay of the data, the encoded authorization code is decoded by the SAM module by means of the personal identity code. The decoded authorization code is then compared with the authorization code stored (non-encoded) on the SAM module. The descrambling by means of the descrambling keys of the data read out of the mass storage is then enabled only when the authorization codes are identical. Owing to this method, which can be performed using very simple hardware, a personalization of the data

09936615 .092704

on the mass storage is effected. For the non-scrambled replay of the data an authorization code is required which may only be obtained via the SAM module of the authorized user because it is linked with the personal identity code of the authorized user.

In a further development of the method the descrambling keys required for descrambling the data are also encrypted with personal data of the authorized user stored on the SAM module, so that they can be decrypted only when using the appropriate SAM module.

In a further configuration of the method the data is output inseparably with a personal identification of the authorized user when the data is replayed via a suitable replay system. The personal identification may consist of a logo or the like, which in the case of image data is displayed in a corner of the picture field.

The replay system in accordance with the invention for performing the method essentially comprises: a read module for accommodating the mass storage, which is preferably a medium which is adapted to be written to by the user, such as, e.g., a miniaturized hard disk or an optical storage disk adapted to be written to by the user; a card reader for the SAM module; a data conditioning electronics for descrambling the data read out of the mass storage; and an output device for the descrambled data. In order to be able to obtain data via a remote network, for instance from the Internet, preferably a payment system for the conditional access to a data provider via the remote network is additionally provided. The payment system is based on a chip card reader which in the preferred embodiment is designed as a plug-in type PC card in the PCMCIA format.

Further advantages and features of the present invention will be apparent from the following description and from the drawings to which reference is made and in which:

The block diagram as shown in Figure 1 of a replay system for performing the method in accordance with the invention diagrammatically shows the essential components of the system. An interface device accommodated in a compact

DE 100 46 146 A1

housing is generally denoted by reference number 10 and comprises three interfaces 12, 14, 16 for plug-in type components as well as an output terminal 18 for a video output device 20. The interface 12 has a plug-in socket for a mass storage 22 which has a fingerprint sensor 24 on a surface accessible to the user. A first SAM module 26 is a part of the interface 12. A second SAM module is contained in the plug-in type mass storage 22, which may be a miniaturized hard disk or also a semiconductor storage, for instance in FLASH technology.

The interface 14 accommodates a chip card reader 28 in the format of a PC card (abbreviation for PCMCIA card). In conjunction with a chip card 30, also referred to as smart card, the chip card reader 28 constitutes a payment system for the conditional access to a provider of multimedia contents and the like, in particular via the Internet.

Connected to the interface 16 is a modem 32 or a network adapter. Via the modem 32 or the network adapter a remote network may be accessed, more particularly the Internet.

A television set or a monitor is connected to the output terminal 18, which may be designed as a SCART interface.

The replay system may further be fitted with an infrared remote control 34.

An internal processor 36 includes the necessary functionality for descrambling and conditioning of the data read out of the mass storage 22 for the replay on the output device 20. The processor 36 is coupled with a synchronized clock 37, which is a part of a monitoring device by means of which the conditioning of the data for replay is made dependent on a certified time stamp which is recorded on the mass storage 22 with the data.

The method in accordance with the invention is illustrated in the charts of Figures 2, 3 and 4. It substantially consists of three stages. In the first stage of the method, illustrated in Figure 2, a personalization of the data in the mass storage takes place. The process is started by transmitting a system certificate to the

DE 10045764 A1

provider of the data. The data involved is more particularly multimedia information, MMI in short. By the system certificate the replay system identifies itself before the MMI provider as a suitable system. A private key is then received on the part of the MMI provider from the SAM module of the replay system to generate a replay authorization code. The private key involved may be a personal identity code or also compressed data derived from the fingerprint sensor 24, or a combination thereof. The replay authorization code is then stored on the SAM module.

Subsequently, payment is effected by means of the payment system 28, 30, whereupon the MMI data is downloaded in a scrambled form and stored on the MMI mass storage 22. The MMI keys necessary for descrambling the MMI data are thereafter transferred to the SAM module in an encrypted form and stored there. The MMI provider further sends an encrypted watermark which may be stored in the SAM module if the volume of the corresponding data is comparatively small; otherwise, storage is effected in the mass storage. Optionally, a certified time stamp is sent with the MMI data and is recorded on the mass storage 22.

As the last step of the first process stage, an encrypted authorization code is sent by the MMI provider and is stored in the MMI mass storage together with the MMI data.

If the data supplied by the fingerprint sensor is incorporated into the private key, such data may be processed or operated on by the SAM module integrated in the mass storage 22.

The method step as shown in Figure 3 relates to the verification of the replay authorization. To this end, the encrypted authorization code read out of the mass storage is decrypted in the SAM module by means of the private key; the authorization code retrieved in this manner is then compared with the authorization code stored on the SAM module. In case the authorization codes are identical, the replay process will be enabled.

EP 0 935 446 A2

In the replay process as illustrated in Figure 4, first the MMI key is decrypted in the SAM module by means of the private key. Then the MMI data is read out of the mass storage and is descrambled by means of the decrypted MMI key. The descrambled MMI data is then overlaid with the personal logo or the watermark and supplied to the output device.

Due to the certified time stamp optionally recorded with the MMI data the permitted replay of the data can be limited in time.

EP 0 966 165 A2

Claims

1. A method of securing data in a portable mass storage against unauthorized copying, in particular for the protection of multimedia information and software, characterized in that:

(a) the data is stored in the mass storage in a scrambled form;

(b) in a replay system for the data at least one personal SAM module is used which has stored thereon a personal identity code of the authorized user;

(c) at least one descrambling key required for descrambling the data is stored on the SAM module of the authorized user;

(d) an authorization code is assigned to the data and is stored on the SAM module;

(e) an authorization code encoded by means of the personal identity code is formed on the SAM module;

(f) the encoded authorization code is stored on the mass storage;

(g) prior to a replay of the data, the encoded authorization code is decoded by the SAM module by means of the personal identity code;

(h) the decoded authorization code is compared with the authorization code stored on the SAM module, and descrambling by means of the descrambling key of the data read out of the mass storage is enabled only when the authorization codes are identical.

2. The method according to claim 1, characterized in that prior to the purchase of the data from a provider, a system certificate is transmitted from the SAM module to the provider and verified by the latter.

DE 100 56 445 A1

3. The method according to claim 1 or 2, characterized in that a session key is used for the secured transfer of the authorization code to the SAM module of the authorized user.

4. The method according to any of the preceding claims, characterized in that for personalizing the data on the mass storage an identification consisting of personal features of the authorized user is formed and linked with the data in such a manner that the data can be output only with the identification.

5. The method according to any of the preceding claims, characterized in that the personal identity code of the authorized user is formed at least in part from data supplied by a fingerprint sensor.

6. The method according to any of the preceding claims, characterized in that the mass storage is arranged in a module adapted to be plugged into a replay system.

7. The method according to claims 5 and 6, characterized in that the fingerprint sensor is arranged on a surface of the plug-in type module.

8. The method according to any of the preceding claims, characterized in that the communication and transaction with the provider of the data is conducted by means of a first SAM module arranged in the replay system, and the personalization of the data is carried out by means of a second SAM module assigned to the mass storage.

9. The method according to claims 6 and 8, characterized in that the SAM module assigned to the mass storage is integrated in the plug-in type module.

10. The method according to any of the preceding claims, characterized in that the mass storage is configured as a miniaturized hard disk.

11. The method according to any of claims 1 to 9, characterized in that the mass storage is configured as flash semiconductor storage.

DE 10054754 A1

12. The method according to claim 11, characterized in that the flash semiconductor storage is removably arranged in an interface module adapted to be plugged into the replay system.

13. The method according to claim 12, characterized in that the interface module comprises a SAM card reader.

14. The method according to any of the preceding claims, characterized in that for purchasing the data a communication and transaction with a provider is effected by means of a remote access to a network.

15. The method according to claim 14, characterized in that the transaction with the provider is effected using a card reader module which is adapted to be plugged into the replay system and which includes a chip card reader and a SAM card reader accommodating the at least one SAM module.

16. The method according to any of the preceding claims, characterized in that the descrambling key is for its part encrypted with personal data stored on the SAM module and is decrypted with such data during replay.

17. The method according to any of the preceding claims, characterized in that a certified time stamp is generated and stored with the data on the mass storage.

18. A replay system for performing the method according to any of the preceding claims, characterized by:

- a read module for accommodating the mass storage;

- a card reader for the SAM module;

- a data conditioning electronics for descrambling the data read out of the mass storage; and

- an output device for the descrambled data.

19. The replay system according to claim 16, further characterized by a payment system based on a chip card reader, for conditional access to a data provider via a remote network.

20. The replay system according to claim 17, characterized in that the chip card reader is configured as a plug-in type PC card in the PCMCIA format.

21. The replay system according to any of claims 18 to 20, characterized in that a monitoring device is provided which evaluates a certified time stamp read out of the mass storage with the data.

DE 100 46 465 A1

Fig. 1

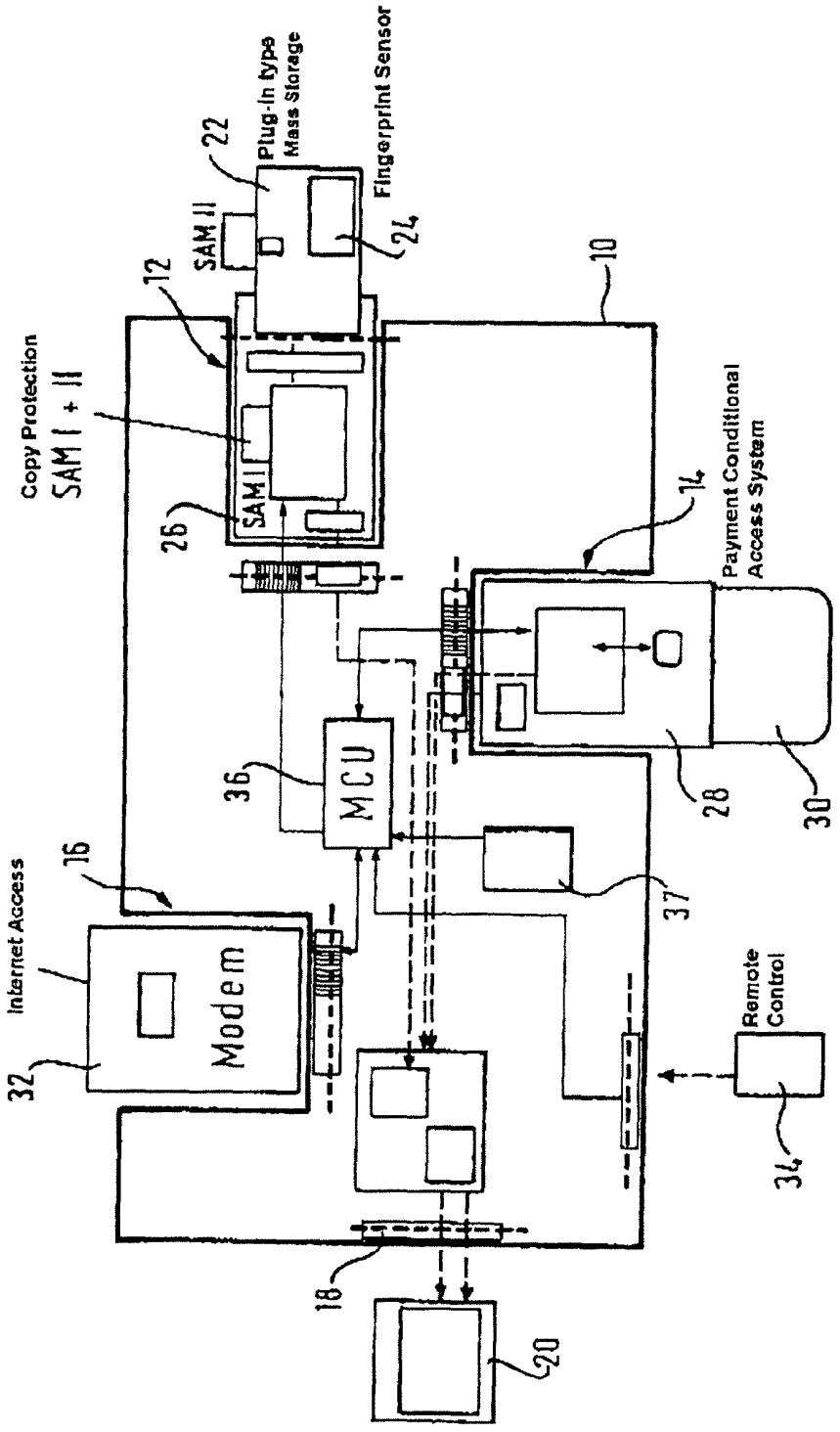

Plug-in type Mass Storage
Fingerprint Sensor
22
SAM II
24
12
10
Copy Protection
SAM I + II
SAM I
26
14
Payment Conditional Access System
36
MCU
28
30
16
37
Internet Access
Modem
32
Remote Control
34
18
20

Fig. 2

Personalization MMI Mass Storage

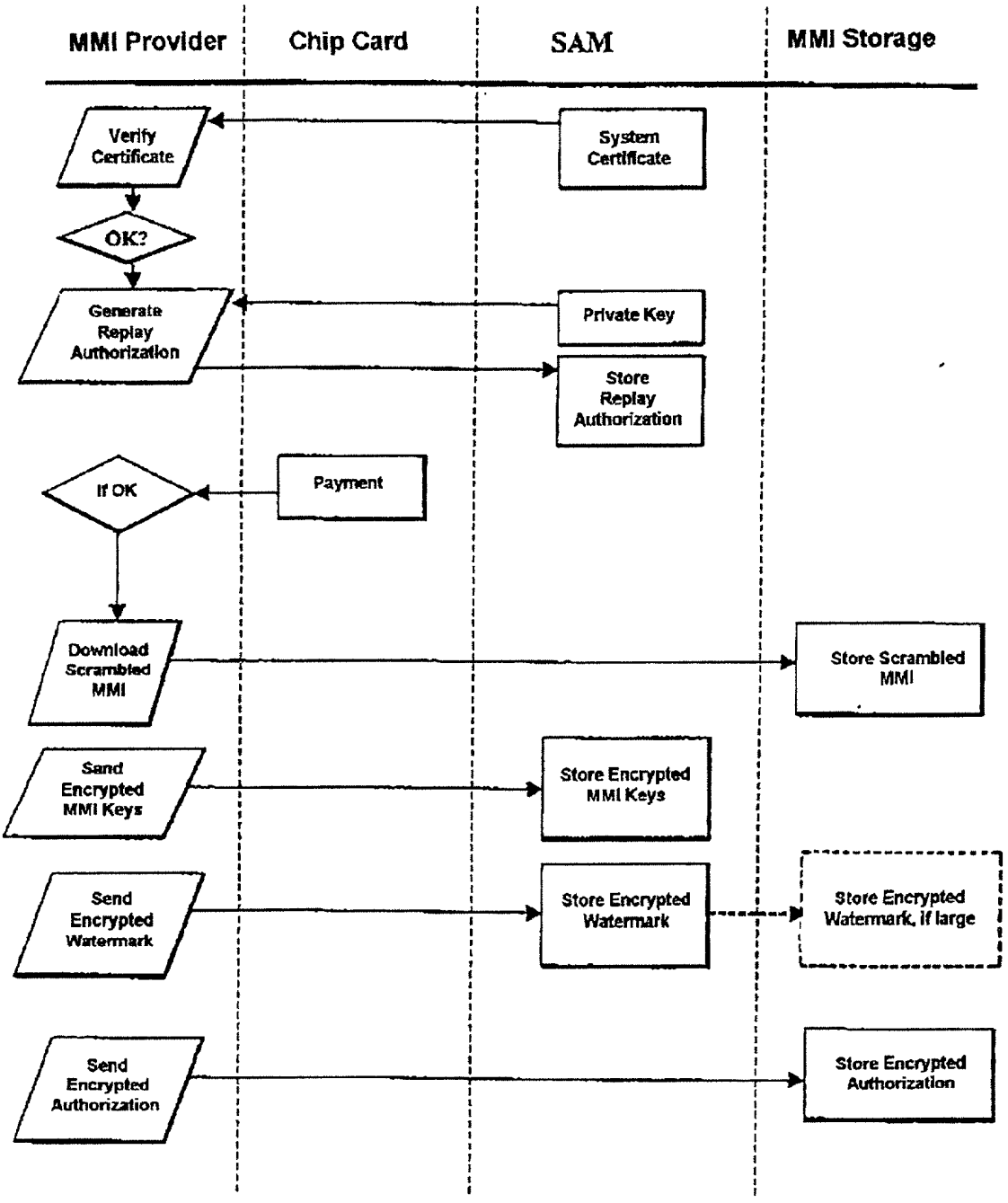
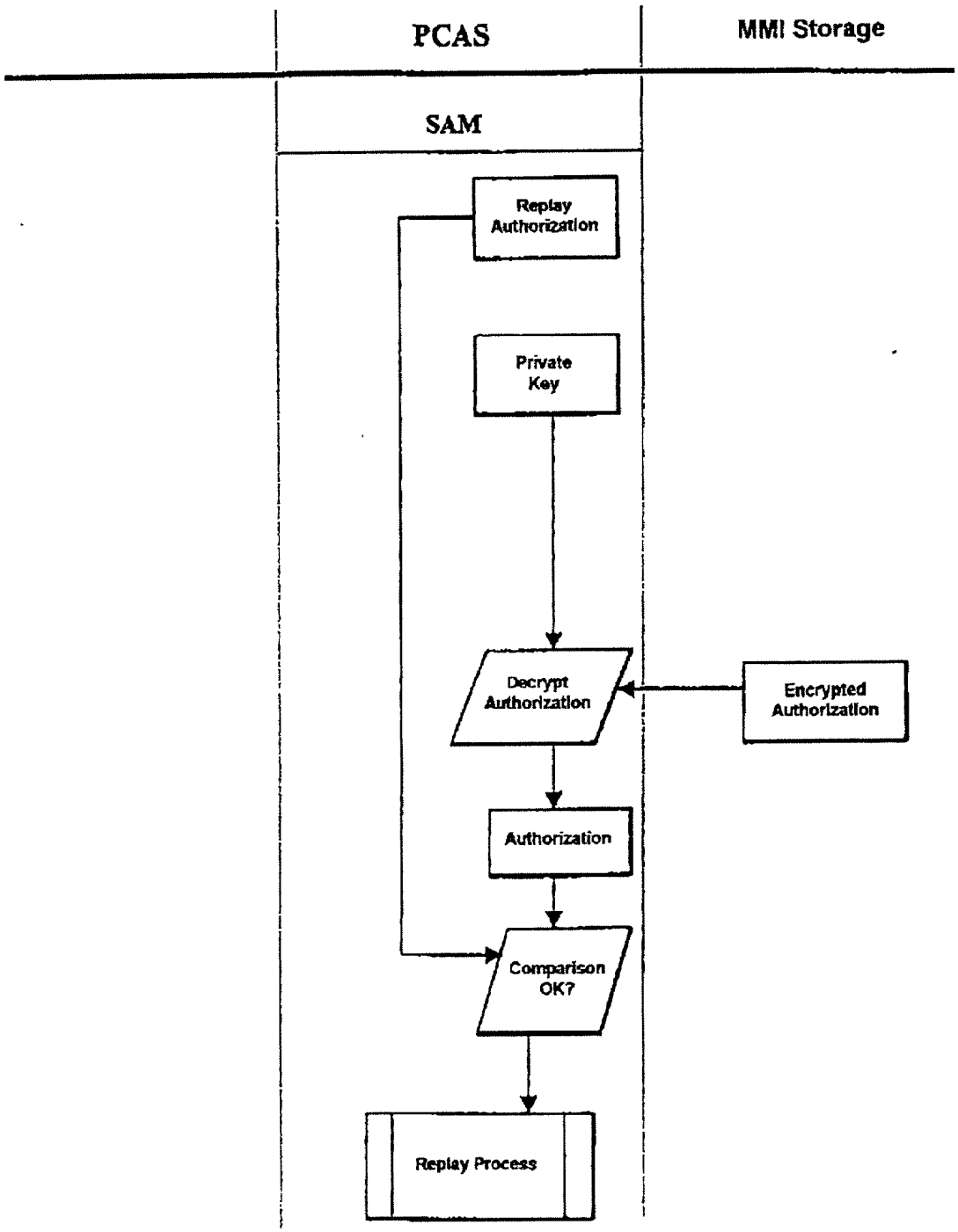


Fig. 3

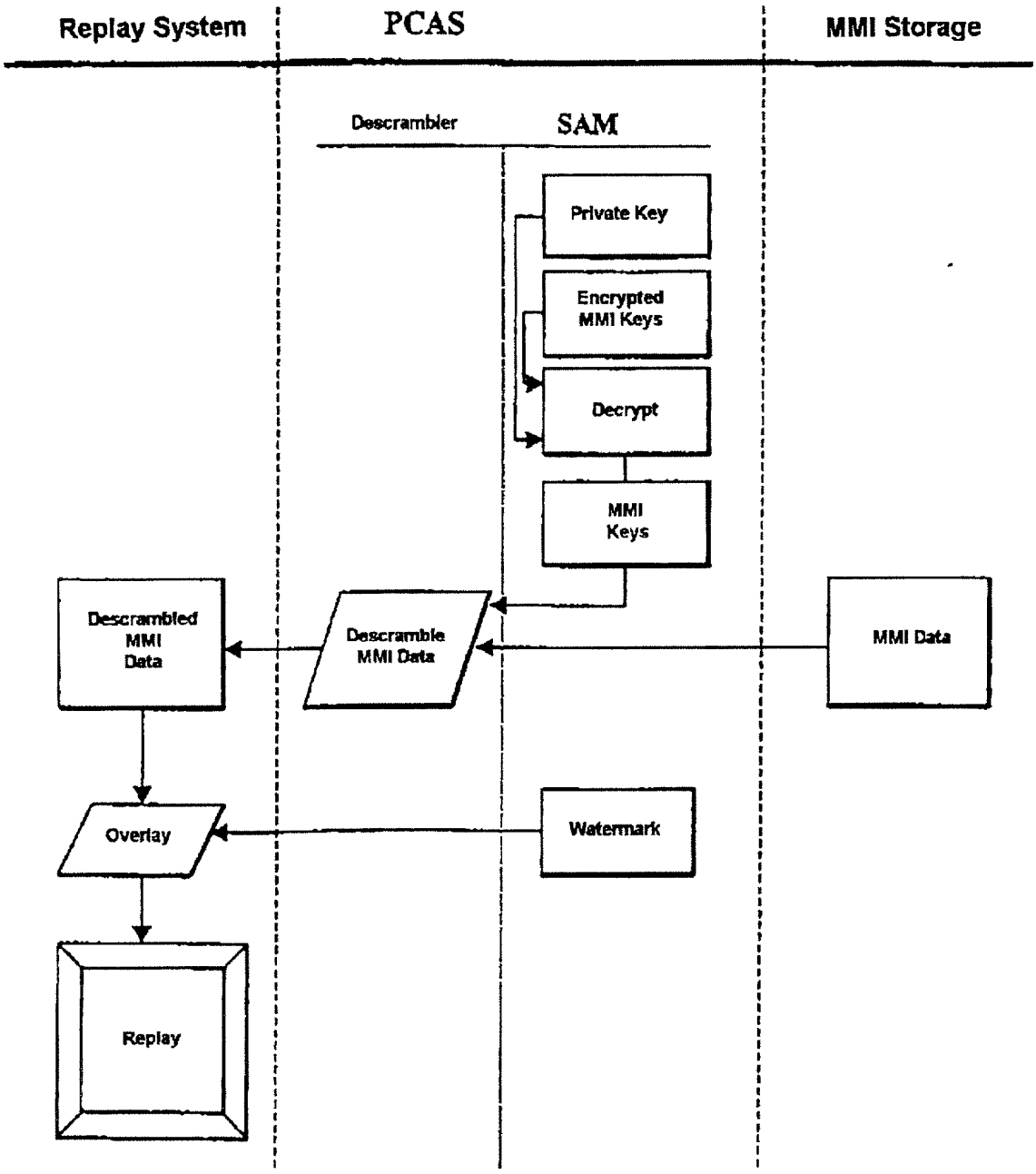
Check Replay Authorization



09936615 - 091401

Fig. 4

Replay Process



Customer Number 22,852
Attorney Docket No. [Text]

DECLARATION AND POWER OF ATTORNEY

As a below named inventor, I hereby declare that: my residence, post office address and citizenship are as stated below next to my name; I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled: [TITLE] the specification of which ☐ is attached and/or ☐ was filed on [Date] as United States Application Serial No. [Text] or PCT International Application No. [Text] and was amended on [Text] (if applicable).

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above. I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56.

I hereby claim foreign priority benefits under 35 U.S.C § 119(a)-(d) or § 365(b) of any foreign application(s) for patent or inventor's certificate or § 365(a) of any PCT international application(s) designating at least one country other than the United States, listed below and have also identified below, any foreign application(s) for patent or inventor's certificate, or any PCT international application(s) having a filing date before that of the application(s) of which priority is claimed:

Country	Application Number	Date of Filing	Priority Claimed Under 35 U.S.C. 119
[Text] Germany	[Text] 199 12 224.5	[Date] 18/03/99	☒ YES ☐ NO
[Text]	[Text]	[Date]	☐ YES ☐ NO

I hereby claim the benefit under 35 U.S.C. § 119(e) of any United States provisional application(s) listed below:

Application Number	Date of Filing
[Text]	[Date]
[Text]	[Date]

I hereby claim the benefit under 35 U.S.C. § 120 of any United States application(s) or § 365(c) of any PCT International application(s) designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application(s) in the manner provided by the first paragraph of 35 U.S.C. § 112, I acknowledge the duty to disclose information which is material to patentability as defined in 37 CFR § 1.56 which became available between the filing date of the prior application(s) and the national or PCT International filing date of this application:

Application Number	Date of Filing	Status (Patented, Pending, Abandoned)
[Text] PCT/EP00/02414	[Text] 17 March 2000	[Text]

I hereby appoint the following attorney and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P., CUSTOMER NUMBER 22,852 Douglas B. Henderson, Reg. No. 20,291; Ford F. Farabow, Jr., Reg. No. 20,630; Arthur S. Garrett, Reg. No. 20,338; Donald R. Dunner, Reg. No. 19,073; Brian G. Brunsvold, Reg. No. 22,593; Tipton D. Jennings, IV, Reg. No. 20,845; Jerry D. Voight, Reg. No. 23,020; Laurence R. Hefter, Reg. No. 20,827; Kenneth E. Payne, Reg. No. 23,096; Herbert H. Mintz, Reg. No. 26,691; C. Larry O'Rourke, Reg. No. 26,014; Albert J. Santorelli, Reg. No. 22,610; Michael C. Elmer, Reg. No. 25,857; Richard H. Smith, Reg. No. 20,609; Stephen L. Peterson, Reg. No. 26,325; John M. Romary, Reg. No. 26,331; Bruce C. Zotter, Reg. No. 27,680; Dennis P. O'Reilley, Reg. No. 27,932; Allen M. Sokal, Reg. No. 26,695; Robert D. Bajefsky, Reg. No. 25,387; Richard L. Stroup, Reg. No. 28,478; David W. Hill, Reg. No. 28,220; Thomas L. Irving, Reg. No. 28,619; Charles E. Lipsey, Reg. No. 28,165; Thomas W. Winland, Reg. No. 27,605; Basil J. Lewris, Reg. No. 28,918; Martin I. Fuchs, Reg. No. 28,508; E. Robert Yoches, Reg. No. 30,120; Barry W. Graham, Reg. No. 29,924; Susan Haberman Griffen, Reg. No. 30,907; Richard B. Racine, Reg. No. 30,415; Thomas H. Jenkins, Reg. No. 30,857; Robert E. Converse, Jr., Reg. No. 27,432; Clair X. Mullen, Jr., Reg. No. 20,348; Christopher P. Foley, Reg. No. 31,354; John C. Paul, Reg. No. 30,413; Roger D. Taylor, Reg. No. 28,992; David M. Kelly, Reg. No. 30,953; Kenneth J. Meyers, Reg. No. 25,146; Carol P. Einaudi, Reg. No. 32,220; Walter Y. Boyd, Jr., Reg. No. 31,738; Steven M. Anzalone, Reg. No. 32,095; Jean B. Fordis, Reg. No. 32,984; Barbara C. McCurdy, Reg No. 32,120; James K. Hammond, Reg. No. 31,964; Richard V. Burgujian, Reg. No. 31,744; J. Michael Jakes, Reg. No. 32,824; Thomas W. Banks, Reg No. 32,719; Christopher P. Isaac, Reg. No. 32,616; Bryan C. Diner, Reg. No. 32,409; M. Paul Barker, Reg. No. 32,013; Andrew Chanho Sonu, Reg. No. 33,457; David S. Forman, Reg. No. 33,694; Vincent P. Kovalick, Reg. No. 32,867; James W. Edmondson, Reg. No. 33,871; Michael R. McGurk, Reg. No. 32,045; Joann M. Neth, Reg. No. 36,363; Gerson S. Panitch, Reg. No. 33,751; Cheri M. Taylor, Reg. No. 33,216; Charles E. Van Horn, Reg. No. 40,266; Linda A. Wadler, Reg. No. 33,218; Jeffrey A. Berkowitz, Reg. No. 36,743; Michael R. Kelly, Reg. No. 33,921; James B. Monroe, Reg. No. 33,971; Doris Johnson Hines, Reg. No. 34,629; Allen R. Jensen, Reg. No. 28,224; Lori Ann Johnson, Reg. No. 34,498; and David A. Manspeizer, Reg. No. 37,540; and Martin F. Majestic, Reg. No. 25,895. Please address all correspondence to FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P., 1300 I Street, N.W., Washington, D.C. 20005, Telephone No. (202) 408-4000.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application or any patent issuing thereon.

Full Name of First Inventor	Inventor's Signature	Date
[Text] Wolfgang NEIFER		Sept. 10, 2001
Residence [Text] 85356 Freising, Germany		Citizenship [Text] German
Post Office Address [Text] Altenhauserstrasse 13, 85356 Freising, Germany		